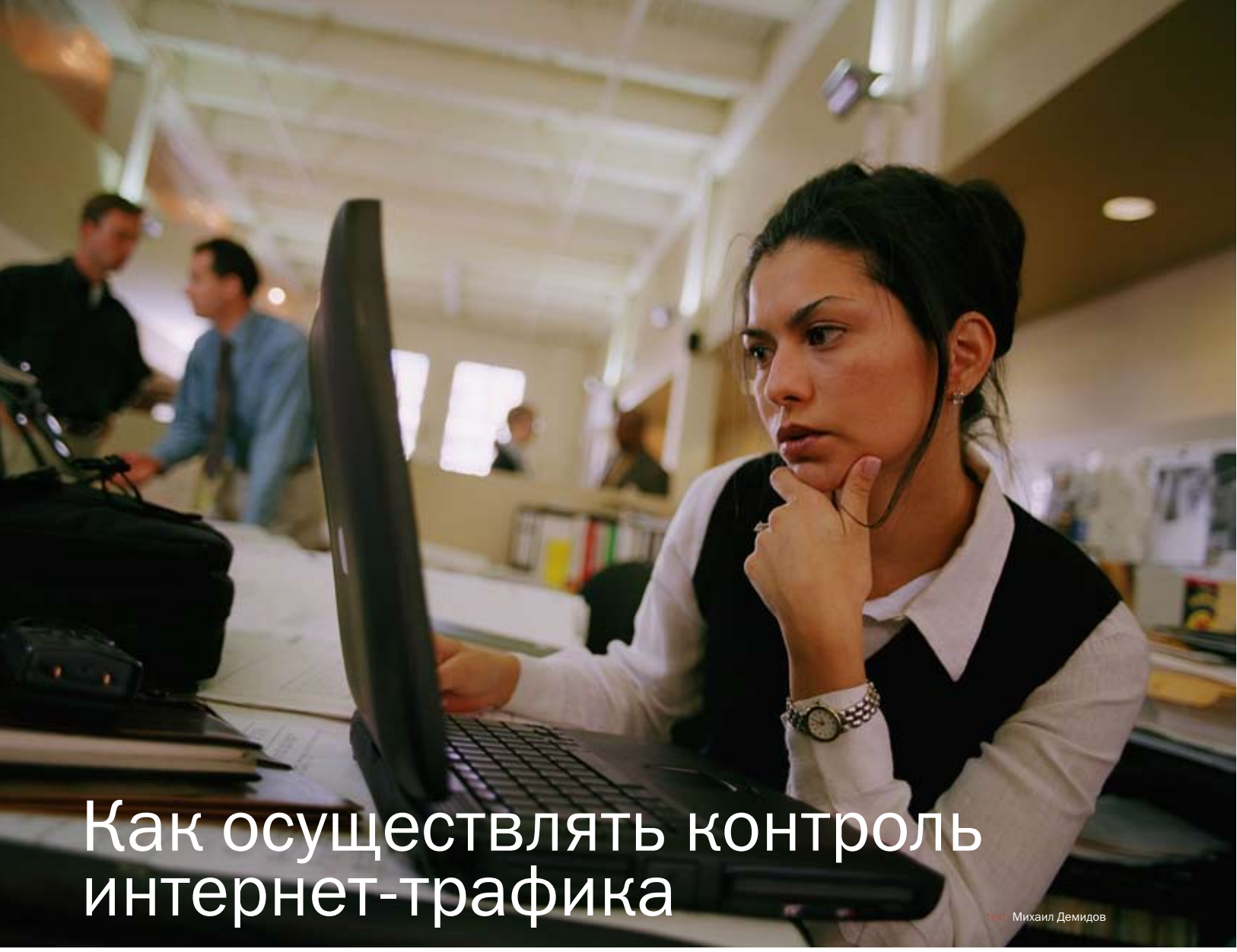


Как осуществлять контроль интернет-трафика

text: Михаил Демидов

Статья отвечает на вопросы:

- Зачем учитывать интернет-трафик
- Как Интернет связан с рациональным использованием рабочего времени сотрудников
- Как оптимизировать нагрузку ЛВС
- Какие задачи решают программы контроля интернет-трафика
- Средства контроля интернет-трафика на уровне малого предприятия

Зачем учитывать интернет-трафик

Представить себе современную компанию, профиль деятельности которой связан с общением с клиентами, чье присутствие в Интернете (хотя бы на уровне качественно работающего сайта-визитки) — жизненно необходимая потребность и чьи бизнес-процессы в той или иной мере связаны с использованием доступа в Интернет, представить, что такая фирма не будет следить за расходом сетевого трафика, сложно. Дело не в том, что многие предприятия малого бизнеса экономят на подключениях, а в том, что каким бы скоростным ни был канал передачи данных, неконтролируемое его использование сотрудниками может серьезно затруднить доступ в Сеть и в некоторых случаях нанести ущерб имиджу компании. Работники под видом исполнения своих обязанностей могут обменяться по электронной почте объемными архивами личных фотографий, загружать из Интернета видеоролики в высоком разрешении или даже скачивать файлы через файлообменные сети, пользуясь возможностями бесплатного для них (но не для предприятия) Интернета. Кроме того, хорошо, если служащий компании при этом не сильно отвлекается от своих прямых обязанностей, а если (как утверждает статистика) на одну только личную переписку по почте у него тратится 1–2 часа рабочего времени? А если этим занимается не один член коллектива, а сразу несколько? В подобных случаях проблема учета расхода сетевого трафика стоит остро.

Как Интернет связан с рациональным использованием рабочего времени сотрудников

С конца 1990-х годов эксперты-психологи начали выделять непродуктивную деятельность сотрудников на рабочем месте, оснащенном выходом в Интернет, и обозначать ее понятием виртуальное безделье (cyberloafing). Изначально термин применялся к тем работникам, которые

СЛОВАРЬ ТЕРМИНОВ

Трафик — в компьютерной технике: объем информации, передаваемой по сети.

Канал передачи данных — часть коммуникационной сети, состоящая из технических средств передачи и приема данных, включая линию связи, а также из средств программного обеспечения и протоколов.

NAT (Network Address Translation) — механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

NAT-драйвер или NAT-сервер — способ подключения локальной сети к Интернету. NAT-драйвер работает на уровне стека протоколов TCP/IP.

Прокси-сервер — способ подключения локальной сети к Интернету. Прокси-сервер работает на уровне приложений.

IP-адрес — уникальный идентификатор (адрес) устройства (обычно компьютера), подключенного к локальной сети или Интернету.

ActiveDirectory — реализация интеллектуальной службы каталогов Microsoft для операционных систем семейства Windows. Позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды.

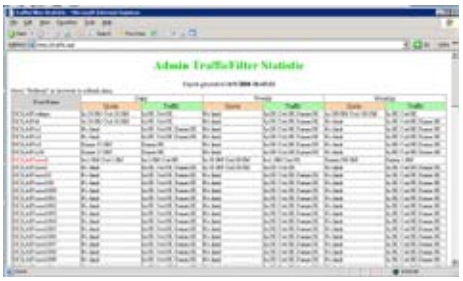
нием дел в статистике использования доступа в Интернет.

Как оптимизировать нагрузку ЛВС

Учет трафика важен и с другой точки зрения, а именно с позиции оптимизации нагрузки на локальную вычислительную сеть (ЛВС). Многие веб-сервисы (хостинги HD-видео, игры жанра MMPORG, файлообменные сети) агрессивно потребляют трафик, что, естественно, сказывается на нагрузке на общий канал доступа. В итоге например развернутые на мощностях самой компании веб-сервер и почтовый сервер могут банально «встать». То есть приложения для учета трафика исполняют роль некоторого защитного механизма (вроде предохранителей в электрощитке), с помощью которого можно добиться повышения стабильности задействованных в компании ключевых решений, использующих интернет-соединения.

Какие задачи решают программы контроля интернет-трафика

Во-первых, программные продукты для контроля трафика для организаций обеспечивают физический учет в виде статистики, а также генерируют аналитические отчеты, на основе которых ИТ-служба и менеджмент компании могут принимать стратегические

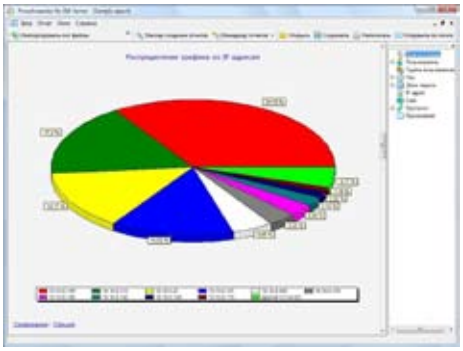


TrafficFilter
Модуль управления интегрируется в оснастку управления ISA Server, есть удаленное администрирование

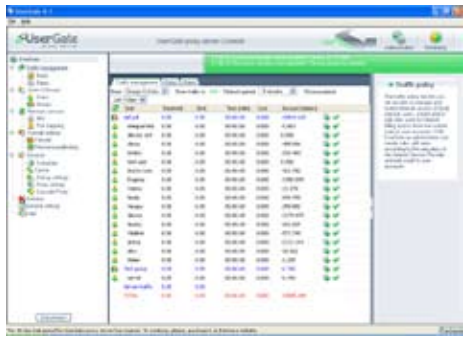
решения (например выбор провайдера связи или рациональное использование рабочего времени). Во-вторых, учет трафика связан с его разделением между приложениями в ЛВС (понятно, что на одном канале могут находиться жизненно важные для бизнеса VoIP и электронная почта, которые подобный продукт должен защищать от возможных сбоев). В-третьих, помимо учета трафика, важно защитить ЛВС организации от потенциальных угроз (утечек данных и внешних атак).

Подобные решения работают на основе трех методов — перехвата пакетов, анализа логов и авторизации. Наиболее распространен первый, поскольку для его осуществления требуется всего лишь установка приложения непосредственно на сервер или шлюз,

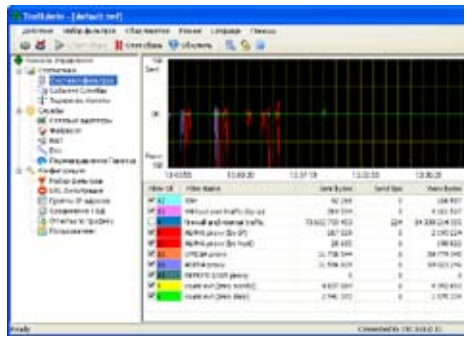
не имели дома дешевого и скоростного подключения к Сети, поэтому использовали рабочий компьютер для проверки и отправки личных почтовых сообщений, скачивания файлов и для веб-серфинга (то есть в основном их деятельность была пассивной). Позже, с развитием социального веба (блогов, социальных сетей и других медиасервисов), «бездельники» стали проявлять себя более активно, что не заставило сказаться на производительности труда и привело к запрещению подобных ресурсов во многих учреждениях. Однако полностью перекрывать доступ к подобным сайтам не совсем правильно — таким образом компания лишается динамично растущего количества клиентов, к тому же данные меры не сказываются положительно на лояльности работников к фирме. Гораздо проще найти компромисс — выделить каждому сотруднику месячную квоту трафика, после превышения которой он будет вынужден отчитаться о том, как это произошло, а служба персонала (или руководство) сможет сверить его объяснения с реальным положе-



■ **Proxy Inspector**
расширенная работа с отчетами



■ **UserGate**
инструменты для фильтрации контента, наличие антивируса



■ **TMeter**
компактный размер, простота настройки, ограничитель трафика

Предприятия СМБ знают о рисках ИБ, но не принимают мер для защиты информации

●●◐ Компания Symantec опубликовала результаты исследования «Хранение данных и безопасность на предприятиях малого и среднего бизнеса», основанного на опросе 1425-ти предприятий в 17-ти странах, который проводился в I квартале 2009 года. Несмотря на понимание рисков для их безопасности, на удивление большое число предприятий СМБ пренебрегает элементарными средствами защиты. Например, три из пяти 59%) фирм этой категории не установили систему защиты персональных компьютеров (программное обеспечение, которое защищает от вредоносных программ). 42% не используют решения для защиты от спама. Почти половина не создает резервные копии своих ПК, подвергая свою информацию серьезному риску. Наконец, треть предприятий не имеет антивируса.
Согласно исследованию, потери предприятий СМБ, связанные с ИТ, можно было бы предотвратить посредством простейших защитных мер. Наиболее распространенной причиной потерь было нарушение работы системы или отказ оборудования. Установка решений резервного копирования для настольных ПК и серверов — простая задача. И ее исполнение обеспечило бы превосходную защиту в подобных случаях.
Исследование показало, что дефицит кадров и средств — два ключевых фактора, вынуждающих предприятия СМБ оставаться беззащитными. 42% фирм не имеют выделенного ИТ-персонала (либо никто не занимается компьютерами, либо ИТ-сотрудник выполняет работу по совместительству). Помехой обеспечению безопасности предприятия считают недостаток квалификации работников 41%). Упоминают также незнание современных угроз 33%) и недостаток времени 28%). Еще один фактор — недостаток средств. Средний бюджет ИТ-безопасности предприятия СМБ составил $4500 в год. Однако заметна тенденция к росту ИТ-бюджета. 50% респондентов сообщили, что в ближайшие 12 месяцев планируют увеличить расходы на безопасность ИТ и хранение данных.

после чего информация об адресатах и отправителях пакетов начинает сохраняться в базе данных. Суммирование записей за определенный период и соотнесение адресата с реальным пользователем системы позволит получить информацию о потреблении трафика этим пользователем. Можно получать точный и адекватный результат, если решение не сильно округляет значения (используется не стандартный, а собственный NAT-драйвер), а также если оно правильно настроено. Другой вариант заключается в анализе журналов, которые создаются при работе прокси-серверов. Качество результатов в этом случае зависит от качества самих логов, поэтому чаще всего такой вариант дополняется подсчетом интернет-пакетов. Третий метод учета трафика связан с использованием авторизаций пользователя (различные варианты — от связки «логин + пароль» или IP-адрес до комбинированной «IP-адрес + MAC-адрес + логин» или через ActiveDirectory). Для правильного учета на рабочих станциях должен быть установлен агент, разрешающий доступ пользователям к интернет-соединению, а в файерволе прописаны соединения по необходимым портам.

Средства контроля интернет-трафика на уровне малого предприятия

Решения, которые могут использоваться для учета трафика, можно разделить на несколько видов:

- надстройки на межсетевые экраны (например на Microsoft ISA Server)
- корпоративные прокси-серверы с собственными NAT-драйверами с функциями по учету трафика
- межсетевые экраны с возможностью разграничения трафика по приложениям.

К первым можно отнести решение TrafficFilter (приложение для Microsoft ISA Server). Оно полностью интегрируется в ISA Server, имеет консоль удаленного управления и не требует установки дополнительных агентов на рабочие станции. Администратор может создавать политики для пользователей/групп пользователей, а также правила квотирования доступа (пользователи могут в режиме реального времени отслеживать состояние своих счетчиков трафика). Кроме того, существует расширение TrafficQuota, позволяющее регулировать доступ в Интернет на основе выделяемой квоты на определенный период времени. Другой продукт для сбора статистики с ISA Server и других серверов — Proxy Inspector. В нем можно увидеть список самых активных рабочих станций в сети, перечень посещаемых ресурсов, получить общее представление о распределении трафика по сайтам, протоколам, дням недели и времени суток. Похожие функции реализованы и в Internet Access Monitor.

Среди корпоративных прокси-серверов упоминания заслуживает решение UserGate, объединяющее в себе кеширующий прокси, файервол с собственным NAT-драйвером, счетчик трафика и сетевой антивирус (для проверки трафика). Статистическая информация о расходе трафика дополняется гибкими инструментами по настройке доступа не только определенной группе пользователей, но и в конкретные промежутки времени (например по будням в рабочие часы), ограничителем скорости доступа, а также продвинутым инструментом для фильтрации контента (рекламы, загрузчика файлов, мониторинга URL). Ближайшие конкуренты UserGate — Kerio WinRoute Firewall, WinGate и NetworkShield Firewall. В первом продукте присутствуют мощные функции по фильтрации нежелательного контента (к примеру, веб-страниц с ключевыми словами, попадающими под действие правила) и модуль статистики Kerio StaR, который выводит разные виды отчетов. Администратор может легко создавать необходимые правила и выставлять квоты потребления трафика, правда, просмотр статистики выполнен отчасти неудобно. Поддерживаются всевозможные варианты доступа в Интернет

Таблица. Сравнительные характеристики средств контроля трафика

Решение	Файервол на уровне приложений	Антивирус	Веб-сайт	Цена (за 50 рабочих станций)	Плюсы	Минусы
TrafficFilter	нет	нет	http://www.isaserver.com.ru/	159/169 евро, до 5 пользователей — бесплатно	Модуль управления интегрируется в оснастку управления ISA Server, есть удаленное администрирование, не требуется установка дополнительного программное обеспечение на машины в ЛВС	требуется наличие ISA Server, нет контроля по приложениям
TrafficQuota	нет	нет	http://www.digirain.com/ru/	299 евро, до 5 пользователей — бесплатно	Экономное использование ресурсов сервера (памяти и процессора), поддержка многопроцессорных систем, интеграция в оснастку ISA Server, предустановленные шаблоны отчетов	требуется наличие ISA Server, нет контроля по приложениям
Proxy Inspector	нет	нет	http://www.advsoft.ru/products/proxyinspector/	14999 рублей за 1 ISA Server	расширенная работа с отчетами (средства автоматизации импорта и создания отчетов, печать из встроенного HTML браузера, экспорт отчетов в Microsoft Excel)	нет дополнительного модуля по перехвату пакетов, требуется наличие ISA Server
Internet Access Monitor	нет	нет	http://www.redline-software.com/rus/products/iam/	4990 рублей	поддержка всех современных прокси-серверов	нет дополнительного модуля по перехвату пакетов
UserGate Proxy&Firewall	есть	есть	http://www.usergate.ru/	15918 рублей (без антивируса)	инструменты для фильтрации контента (реклама, типы файлов), наличие антивируса, собственный NAT-драйвер	достаточно сложная система правил
Kerio WinRoute Firewall	есть	есть	http://www.kerio.ru/	1067 евро (без антивируса)	инструменты для фильтрации контента (реклама, типы файлов), расширенная статистика	необходимость покупки дополнительных лицензий для фильтрации контента
WinGate	есть	есть	http://www.qbik.com/products/wingate/index.php	825/1120 долларов в зависимости от версии	встроенный почтовый сервер для учета почты, расширенная сетевая поддержка	высокая стоимость
NetworkShield Firewall	есть	нет	http://www.networkshield.ru	13850 рублей	удобный подсчет и анализ соединений, поддержка учета по авторизации, низкие системные требования	нет расширений
BWMeter	нет	нет	http://www.desksoft.com/BWMeter.htm	30 долл.	компактный размер, простота настройки	нет расширений
TMeter	нет	нет	http://www.tmeter.ru/	1996 руб (40 фильтров трафика)	компактный размер, простота настройки, ограничитель трафика	учет по фильтрам, отсутствие файервола уровня приложений
Интернет Контроль Сервер	нет	нет	http://xserver.a-real.ru/	17300 рублей	встроенный почтовый сервер для учета почты, расширенная сетевая поддержка	высокая стоимость
Traffic Inspector	есть	есть	http://www.smart-soft.ru/	10800 рублей	низкая стоимость	использование стандартного NAT-драйвера

и авторизации. WinGate во многом повторяет функциональность UserGate, но имеет встроенный почтовый сервер для учета почтового трафика и расширенную поддержку сетевых экранов для различных операционных систем, в том числе MacOS и Linux, без необходимости установки дополнительных клиентских программ. В NetworkShield Firewall учету трафика выделено довольно много внимания — система квотирования и разделения правил трафика реализована на высоком уровне. Плюс ко всему, программа позволяет отслеживать в реальном времени активность объектов в Сети на основе сессий и соединений.

Более простыми решениями для подсчета интернет-трафика являются утилиты: BWMeter, устанавливающаяся в качестве службы и отслеживающая пакеты во всех соединениях на компьютерах ЛВС с возможностью фильтрации и ограничения трафика; TMeter, выполняющая те же функции, но поставляющаяся еще и как freeware-решение (количество фильтров не превышает трех, в то время как в платных редакциях утилиты их намного больше).

Если же пользователю необходимо комплексное решение, которое содержит в себе всю необходимую функциональность для управления трафиком, можно воспользоваться «Интернет Контроль Сервером». Данный продукт представляет собой маршрутизатор со встроенными HTTP-прокси-сервером (Squid) и сервером электронной почты SMTP (Postfix), работающий на базе FreeBSD. Комплексным решением считается и Traffic Inspector — в нем функциональность кэширующего прокси-сервера с антивирусом дополняется биллинговой системой, которая ведет точный детализированный учет, по всем пользователям и по внешним каналам подключения к провайдерам.

■ **Traffic Inspector**
низкая стоимость

Выводы

Внедрение подобных решений требует достаточно серьезного обоснования, поскольку рассмотренные в материале продукты являются коммерческим программным обеспечением, стоимость которого может превышать возможную экономию от снижения потребления интернет-трафика. Кроме того, для использования этих программ придется подготовить соответствующую среду. С точки зрения юзабилити наиболее удобны те решения, чей дистрибутив содержит все необходимые компоненты и утилиты, которые конфигурируются уже в процессе установки, а не стыкуются после нее. К тому же это займет меньше времени и сил, чем при установке всех компонентов по отдельности. В основе такие решения имеют open source систему, например Linux или FreeBSD, поэтому расходы на приобретение программного обеспечения для развертывания счетчика трафика сводятся к нулю. Еще одно преимущество подобных решений — реализация консоли управления через веб-интерфейс, что означает простоту в управлении и не требует обучения сотрудника ИТ-службы. Коммерческие решения на базе Microsoft подразумевают, что компания приобретает серверную операционную систему от Microsoft, СУБД (например Microsoft SQL), межсетевой экран (Microsoft ISA Server), а также обучает системного администратора работе с этими продуктами.

Еще одна сложность во внедрении систем учета трафиком заключается в том, что их необходимо встраивать в существующую ИТ-инфраструктуру средств информационной безопасности. Отчасти этот момент продуман в продуктах, имеющих антивирусную составляющую (UserGate, WinGate, Traffic Inspector, Kerio WinRoute Firewall), однако вопрос совместимости систем между собой должен решаться индивидуально. ◑●●

Четвертое поколение продуктов ESET NOD32

●●◐ Компания ESET сообщила о начале продаж четвертой версии антивирусных продуктов ESET NOD32 в России и странах СНГ.
Новинки способны надежно защитить конфиденциальные данные пользователей, платежные пароли и логины, обеспечить безопасность каналов связи с системами интернет-банкинга. Они могут сканировать трафик защищенных соединений HTTPS и POP3S, а также почтовые сообщения, получаемые по протоколу IMAP, предотвращая фишинг- и фарминг-атаки.
Контроль использования съемных носителей — флэш-карт, USB-устройств — осуществляется с помощью специального модуля. Можно ограничить доступ к данным устройствам, не прибегая к перенастройке ОС или материнской платы. Благодаря этой возможности сводится к минимуму риск заражения ПК вредоносным ПО, передающимся с помощью внешних носителей.
Решения интегрируются с клиентами электронной почты: Microsoft Outlook Express, Microsoft Windows Mail, Microsoft Windows Live Mail и Mozilla Thunderbird. Также проверяется почтовый трафик по стандартным протоколам, вне зависимости от того, какой почтовый клиент используется.
Интегрированный модуль ESET SysRescue позволяет создавать загрузочный диск или флэш-карту для восстановления системы. Пользователь может загрузить компьютер с данного носителя, просканировать ПК и в случае заражения вылечить.
В модуле защиты от спама появился лист исключений. Находящиеся в нем адреса не могут добавляться в «белый» или «черный» списки и всегда проверяются на наличие спама. Данная мера помогает избежать получения спама, имитирующего письма, отправляемых с известных пользователю адресов. С помощью адресной книги пользователь может самостоятельно управлять списком адресов, которые помечаются как надежные или ненадежные.
Важным новшеством стала способность ESET NOD32 идентифицировать тип ПК пользователя. Если ПК определен как ноутбук, не подключенный к блоку питания, то антивирус автоматически откладывает некоторые запланированные задачи, например загрузки больших обновлений, чтобы сэкономить расход энергии.
В корпоративные решения ESET NOD32 Business Edition добавились поддержка баз данных Microsoft Access, Microsoft SQL Server, MySQL и Oracle, контроль безопасности конечных точек, а также расширенные возможности масштабирования в распределенных сетях. В комплект поставки корпоративных решений входит приложение ESET Remote Administrator — оно позволяет централизованно устанавливать и настраивать продукты ESET в корпоративных сетях.